Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Group 6
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The project is a streaming application for movies and series. The kind of information that will be processed is usernames, passwords, e-mails, payment information, user's preferences and data collected from user's choices.
The processing of this data satisfies the following criteria:
- Evaluation or scoring as well as Systematic monitoring, since we collect data from user's preferences and choices to predict what they may like, so we can present to them in the future;
- Sensitive data or data of highly personal nature, considering that we collect user's preferences, we have in our possession data that may be of personal nature regarding the user.

We identified the need for a DPIA because of the type of information we are dealing with and the need to protect our customer.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Initially we collect data from questions to the users regarding their preferences, their basic information, and we store them in our server a centralized data-base. We only delete data when a user deletes is account. We also collect data from user choices, this data is also stored in a centralized data-base, and is also deleted when the user deletes is account.
The source of the data is always the user, either by answering questions, or by monitoring user interaction.
The data won't be shared with anyone.
The personal information gathered may have high risks involved.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is always user oriented, especially their likes.
All data will be collected concerning user interaction, it will always be collected and stored to make better predictions.
All users are subjected to this processing. And there are no specific geographical area.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The users are clients that are always aware of the collection of the data, they will have to authorize the collection of the data when they register. They can always unsubscribe and all their data gets erased. We don't expect children or other vulnerable groups to subscribe the service.
All information gathered will be submitted to a anonymization process, making it imperceptible to any attacker.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

With our processing we expect to provide a more personal oriented service. We want our customers to discover new things they may like, making them satisfied with our service.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

We want all our experts to be within our trust boundaries. We don't expect to need any third party involved.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The collection of the data is only done with user permission to achieve a better experience when using the application. There is no other way to achieve this goal.
When the data collected is being treated all information concerning user identification will be anonymized to protect the rights of the users.
Processors will be given only the minimal to achieve the purpose.
We don't expect any international transfers.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA